AGREEMENT
on the entrustment of personal data processing

TrustMate S.A with its registered office in Wrocław, ul. Bartoszowicka 3, 51-641 Wrocław, entered in the register of entrepreneurs of the National Court Register kept by the District Court for Wrocław-Fabryczna in Wrocław, VI Commercial Division of the National Court Register under the number 0000737597, NIP 8971854393, REGON 369980751, with a share capital of PLN 2,843,170 fully paid up,
represented by the President of the Management Board Jerzy Krawczyk, authorized to represent the company independently, hereinafter referred to as the ***"Service Provider"***,

and

Company registering an account on TrustMate

The person registering the account declares/declare that:

1. Is authorized to represent the Company individually/jointly,

2. Is authorized to act on behalf of the company.

hereinafter referred to as the "***Service Partner"***,

and collectively referred to as the ***"Parties"***, each individually referred to as the ***"Party"***, with the following content:

§1 Definitions

The terms used in the agreement shall have the following meanings:

1. **Processing Entity** – the entity to which the processing of personal data has been entrusted under the entrustment agreement,
2. **Administrator** – the body, organizational unit, entity, or person that decides on the purposes and means of processing personal data, also referred to as the "Principal",
3. **Data Set** – any structured set of personal data accessible according to specific criteria, whether distributed or functionally divided,
4. **Data Processing** – any operations performed on personal data, such as collecting, recording, storing, processing, changing, sharing, and deleting, especially those performed in information systems,
5. **Regulation** – Regulation of the European Parliament and the Council (EU) 2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation),
6. **Other Processing Entity** – the entity to which the Processing Entity, on behalf of the Administrator, has wholly or partly subcontracted the processing of personal data,

7. **Cooperation Agreement** – means the agreement concluded between the parties under which the Service Provider will perform services involving the processing of personal data on behalf of the Service Partner.

§2 Subject of the Agreement, purpose, nature, and scope

1. The subject of the agreement is the entrustment by the Service Partner of personal data for processing by the Service Provider.
2. The purpose of the entrustment is:
   a. Sending invitations to provide reviews, sending reminders in case of no response to the email invitation, and sending thanks after submitting a review, managed by the Service Partner, in the form of email or text message.
   b. In the case of using the "Advanced Survey Research" module - sending invitations to complete a survey, sending reminders in case of no response to the email invitation, and sending thanks after completing the survey, managed by the Service Partner, in the form of email or text message.
3. The Service Provider is authorized to process personal data solely for purposes related to the performance of Services provided to the Service Partner under the Cooperation Agreement.
4. The nature of processing concerns the processing of personal data using information systems.

§3 Personal data processed by the Contractor

The personal data entrusted to the Service Provider include, among others, data processed in connection with the conclusion, implementation, and settlement of service provision agreements between the Service Partner and its customers, including customer contact data;

§4 Duration of processing

1. The Processing Entity is authorized to process the entrusted data until the purpose of the service, which is receiving a review (or survey - only applies to the use of the "Advanced Survey" module) from a customer or termination of the Agreement,
2. Within 14 days from the termination of the Agreement, the Processing Entity is obliged to delete the entrusted data from all media, programs, and applications, including copies, unless the obligation to further process them results from separate legal provisions.

§5 Duties and rights

1. The Service Provider is obliged to process personal data solely on documented instruction from the Service Partner, which also applies to the transfer of personal data to a third country or an international organization, with documented instructions being considered those transferred electronically or in writing. The above obligation does not

apply when the requirement to process personal data is imposed on the Service Provider by European Union law or Polish law.

2. The Service Provider is responsible for protecting the personal data entrusted to it for processing,
3. The Service Provider takes all measures required under Article 32 of Regulation (EU) 2016/679 to ensure the security of personal data,
4. The Service Provider adheres to the terms of using another processing entity, as referred to in §7 of this agreement,
5. Upon request from the Service Partner, the Service Provider will inform the Service Partner of the location of the Data processing
6. The Service Provider, considering the nature of the processing, is obliged to assist the Service Partner, to the extent possible, by appropriate technical and organizational measures, to fulfill the obligation to respond to requests from the person whose data is concerned, regarding the exercise of their rights as defined in Chapter III of Regulation (EU) 2016/679, especially concerning information and transparent communication, access to data, the duty to inform, the right of access, the right to rectification of data, deletion of data, restriction of processing, data portability, the right to object. For this purpose, the Service Provider is obliged to inform the Service Partner of any request from the entitled person in the course of exercising their rights under Regulation (EU) 2016/679 and to provide the Service Partner with all necessary information in this regard,
7. The Service Provider, considering the nature of the processing and the information available to it, helps the Service Partner fulfill the obligations set out in Articles 32-36 of Regulation (EU) 2016/679,
8. The Service Provider commits to continuously monitor changes in data protection regulations and adjust data processing methods, particularly internal procedures and methods of protecting personal data, to the current legal requirements,
9. The Service Provider is obliged to provide the Service Partner with all information necessary to demonstrate that it fulfills the obligations specified in this article of the agreement and allows the Service Partner or an auditor authorized by it to conduct audits, as mentioned in §9 of this agreement, and contributes to them,
10. In connection with the duty specified in paragraph 9 above, the Service Provider will immediately inform the Service Partner if, in its opinion, the instruction issued to it constitutes a violation of Regulation (EU) 2016/679 or other European Union or Polish data protection regulations,
11. The Service Provider will immediately inform the Service Partner of any proceedings, in particular administrative or judicial, regarding the processing of personal data by the Service Provider, any administrative decision or judgment concerning the processing of Personal Data directed to the Service Provider, as well as any control actions taken against it by the supervisory authority and the results of such a control if its scope included Personal Data entrusted to the Service Provider under this agreement.

§6 Reporting incidents

1. The Service Provider undertakes to report any personal data breach to the Service Partner within 24 hours of detection.
2. The information provided to the Service Partner should include at least:
   a. a description of the nature of the breach and, where possible, the categories and

approximate number of individuals affected and the types/amounts of data involved,
   b. a description of the possible consequences of the breach,
   c. a description of the measures taken or proposed by the Service Provider to address the breach, including measures to mitigate its adverse effects.

§7 Use of another processing entity by the Service Provider

1. The Service Partner agrees to the Service Provider subcontracting the processing of Personal Data to entities that provide IT support for the Service Provider during the term of the cooperation agreement. As of the date of signing the agreement, these are: Amazon Web Services EMEA SARL (38 Avenue John F. Kennedy L-1855 Luxembourg) and Google Cloud Platform https://cloud.google.com/about/locations, EUROPE-CENTRAL2. Subcontracting does not occur to third countries (outside the EEA). The Service Provider chooses suppliers providing a level of protection not lower than specified in the Agreement,
2. The Service Provider is obliged to ensure that any other processing entity it intends to use to process personal data provides adequate guarantees of implementing appropriate technical and organizational measures to meet the requirements of Regulation (EU) 2016/679 and protect the rights of the data subjects,
3. Further subcontracting of processing activities to another processing entity, as mentioned in §7 paragraph 1 of the agreement, is only possible under the condition that the Service Provider imposes on this other processing entity, by contract, the same data protection obligations as those resting on the Service Provider under this agreement, particularly the obligation to implement appropriate technical and organizational measures to ensure that processing meets the requirements of Article 32 of Regulation (EU) 2016/679,
4. If the subcontracting of personal data processing to another processing entity by the Service Provider involves transferring the data to a third country that does not provide an adequate level of personal data protection on its territory and there are no other grounds allowing the transfer of personal data to that third country, the Service Provider will sign an agreement with the processing entity located in such a third country containing:
   a. "Standard Contractual Clauses" adopted under Commission Decision 2010/87/EU of 5 February 2010 on the transfer of personal data from the European Union to third countries, or
   b. "Standard Data Protection Clauses" adopted in accordance with Article 46 paragraphs 2(c) and (d) of Regulation (EU) 2016/679, or authorize in writing the Service Provider to sign the aforementioned agreement on its behalf. Entering into such an agreement with a processing entity located in a third country entitles the Service Provider to use the services of this processing entity in processing Personal Data,
5. The agreement, indicated in paragraph 4 above, is concluded in written form. The requirement of written form is met by an agreement concluded electronically.

§8 Declared technical and organizational measures

1. The Service Provider declares that it has the resources, experience, expertise, and qualified personnel necessary to properly perform this Agreement and implement

appropriate technical and organizational measures, and has fulfilled all the conditions of legality of personal data processing,

2. The Service Provider guarantees that every person executing the Agreement is obligated to ensure the indefinite confidentiality of personal data processed in connection with the execution of the Agreement, especially that they will not transfer, disclose, and make these data available to unauthorized persons. Simultaneously, each person executing the Agreement is obliged to keep the methods of securing personal data secret.
3. The Service Provider declares the use of technical and organizational measures specified in Article 32 of the Regulation, as adequate to the identified risk of violation of rights or freedoms of the entrusted personal data, particularly:
    a. pseudonymization and encryption of personal data,
    b. the ability to ensure continuous confidentiality, integrity, availability, and resilience of processing systems and services,
    c. the ability to restore the availability and access to personal data promptly in the event of a physical or technical incident,
    d. regular testing, assessing, and evaluating the effectiveness of technical and organizational measures to ensure the security of processing.

§9 Audit right

1. The Service Partner is entitled to conduct an audit of personal data processing to verify whether the Service Provider is meeting the obligations specified in this agreement.
2. The parties agree on the following rules for conducting the audit referred to in paragraph 1 above: a. The audit may involve both the demand to present documents and information related to data processing and on control activities carried out at the data processing site during working days (understood as Monday to Friday, excluding Saturdays and public holidays) from 10:00 AM to 4:00 PM, after prior written notification to the Contractor of the audit date and scope, at least 10 days before the start of the audit, b. The Service Partner conducts the audit personally or through independent external auditors authorized to conduct the audit on its behalf.
3. Control activities conducted during the audit referred to in §9, paragraph 3(a), may specifically include:
    a. notes from the activities carried out (particularly notes from received explanations and conducted inspections),
    b. copies of documents and registers concerning data processing,
    c. prints of personal data from information systems,
    d. prints of copies of images displayed on the screens of devices that are part of the information systems used for data processing,
    e. recordings of technical configurations of security systems where data processing takes place. The costs of the aforementioned audit shall be borne by the Principal.
4. The Service Partner provides the Service Provider with a copy of the audit report. If the audit reveals discrepancies in the actions of the Service Provider with the agreement or data protection regulations, the Service Provider shall immediately ensure that the processing of personal data complies with the provisions of the agreement or the regulations violated as stated in the audit report.

§10 Liability of the Parties

1. The Service Provider is liable for the actions and omissions of persons through whom it will process the entrusted personal data, as for its own actions or omissions.
2. The Service Provider is liable for damages incurred by the Service Partner or third parties as a result of non-compliance with this agreement in processing personal data.

§11 Final Provisions

1. This agreement is concluded for the duration of the Cooperation Agreement.
2. Termination of the Main Agreement results in simultaneous termination of this Agreement.
3. If the results of the audit referred to in §9 of this agreement or the control carried out by the supervisory authority at the Service Provider or another processing entity to which the Service Provider has entrusted the processing of personal data demonstrate that the Service Provider has culpably violated the provisions of this agreement, the Principal is entitled to terminate this agreement with immediate effect.
4. In the event of termination of this agreement, depending on the decision of the Service Partner, the Service Provider will delete all personal data and immediately and irreversibly destroy all copies of documents and records on all media containing personal data, unless European Union law or the law of the Republic of Poland requires the Service Provider to continue storing personal data. In such a case, the Service Provider is responsible for processing the aforementioned data after the termination of this agreement as an administrator.
5. Any changes or additions to this agreement require written form under pain of nullity. The requirement of written form is satisfied by sending and accepting written changes or additions to the agreement in electronic form by both Parties.
6. In matters not regulated by this agreement, the provisions of the Civil Code, Regulation (EU) 2016/679, and the Act on Personal Data Protection shall apply.
7. Any disputes arising from the legal relationship covered by this agreement shall be considered by the court competent for the seat of the Service Partner.
8. The agreement is drawn up in two identical copies, one for each of the Parties.
9. The agreement enters into force on the date of signing and supersedes all other arrangements made between the Service Provider and the Service Partner regarding the processing of personal data, regardless of whether they were regulated by an agreement or another legal instrument.
10. In the event of the repeal of the UODO (Personal Data Protection Office) and/or its implementing acts, all references to the Act in this agreement should be treated as references to the relevant provisions of Regulation (EU) 2016/679. To avoid any doubt, the Parties agree that in the event of the repeal of the UODO and/or its implementing acts, they will not be obligated to meet the requirements specified therein.

____________________ ____________________

Service Partner TrustMate